Claims

[1] A network security system for permitting a trusted process using a firewall, the firewall protecting a corresponding network connection of a computer to a network by setting restrictions on information communicated between networks, comprising:

a port monitoring unit for extracting information about a server port being used through a network communication program;

an internal permitted program storage for extracting information about a program for which communication is permitted by the firewall, and registering the extracted information;

an internal permitted port storage, if the port monitoring unit extracts the information about the server port being used using the program registered in the internal permitted program storage, registering the extracted information about the server port; and

a device for making the firewall flexible, determining whether a destination port of a packet of inbound traffic has been registered in the internal permitted port storage, and if the destination port has not been registered, transmitting the corresponding packet to the firewall, and if the destination port has been registered, allowing the corresponding packet to bypass the firewall.

[2] The network security system as set forth in claim 1, wherein the information about the program, which is extracted and registered in the internal permitted program storage, includes information about a program name, an entire path of the program, and a program Message Digest 5 (MD5) hash value.

[3] The network security system as set forth in claim 1, whereinthe information about the server port, which is extracted and registered in the internal permitted port storage, includes information about an entire path of the program, a protocol, and a port.

[4] A network security method of permitting a trusted process using a firewall, the firewall protecting a corresponding network connection of a computer to a network by setting restrictions on information communicated between networks, comprising:

the first step of extracting information about a server port being used through a network communication program;

the second step of extracting information about a program for which com-

munication is permitted by the firewall, and registering the extracted information in an internal permitted program storage;

the third step of, if information about the server port being used is extracted using the program registered in the internal permitted program storage at the first step, registering the information about the extracted server port in internal permitted port storage;

the fourth step of determining whether a destination port of a packet of inbound traffic has been registered in the internal permitted port storage;

the fifth step of, if, as a result of the determination at the fourth step, the destination port has not been registered, transmitting the packet of inbound traffic to the firewall and

the sixth step of, if, as a result of the determination at the fourth step, the destination port has been registered, allowing the corresponding packet to bypass the firewall.

[5] The network security method as set forth in claim 4, wherein, in the case of performing communication using Transmission Control Protocol (TCP), the first step extracts a listen port through hooking when a socket performs Listen to operate as a server.

[6] The network security method as set forth in claim 4, wherein, in the case of communication using User Datagram Protocol (UDP), the first step extracts the server port by performing hooking in a user mode when a socket calls a relevant function to receive a packet.

[7] The network security method as set forth in claim 4, wherein, the sixth step allows the corresponding packet to bypass the firewall by calling a hooked original function.

[8] The network security method as set forth in claim 4, wherein the information about the program, which is extracted and registered at the second step, includes information about a program name, an entire path of the program, and a program Message Digest 5 (MD5) hash value.

[9] The network security method as set forth in claim 4, wherein the information of the server port, which is extracted and registered at the third step, includes information about an entire path of the program, a protocol, and a port.

[10] A computer-readable recording medium for performing a network security method using a firewall, the medium storing a program for executing the method, the method comprising:

the first step of extracting information about a server port being used through a network communication program;

the second step of extracting information about a program for which communication is permitted by the firewall, and registering the extracted information in an internal permitted program storage;

the third step of, if information about the server port being used is extracted using the program registered in the internal permitted program storage at the first step, registering the information about the extracted server port in an internal permitted port storage;

the fourth step of determining whether a destination port of a packet of inbound traffic has been registered in the internal permitted port storage;

the fifth step of, if, as a result of the determination at the fourth step, the destination port has not been registered, transmitting the packet of inbound traffic to the firewall and

the sixth step of, if, as a result of the determination at the fourth step, the destination port has been registered, allowing the corresponding packet to bypass the firewall.